STRATEGY RESEARCH PROJECT

LEVERAGING INFORMATION TECHNOLOGY TO ENABLE ARMY TRANSFORMATION: CAPABILITIES AND CHALLENGES FOR THE INTERIM FORCE

BY

LIEUTENANT COLONEL RANDALL G. CONWAY
United States Army

SENIOR SERVICE COLLEGE FELLOW
AY01

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

LEVERAGING INFORMATION TECHNOLOGY TO ENABLE ARMY TRANSFORMATION: CAPABILITIES AND CHALLENGES FOR THE INTERIM FORCE

by

LIEUTENANT COLONEL RANDALL G. CONWAY
Department of the Army

Colonel Kevin R. Cunningham, PhD
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Randall G. Conway

TITLE: Leveraging Information Technology to Enable Army Transformation: Capabilities and Challenges for the Interim Force

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 54 CLASSIFICATION: Unclassified

The Army is now engaged in a formal transformation process to create forces to capitalize on technological and organizational opportunities that new electronic, automotive, and ballistic technologies appear to provide. The transformation effort is also designed to alleviate problems in strategic mobility that have traditionally degraded the Army's ability to rapidly deploy forces other than light and airborne infantry. The transformation process will move along three interdependent yet simultaneous axes: the Legacy Force, the Interim Force, and the Objective Force. The purpose of this study is to examine the Interim Force and determine whether or not the higher technical performance expected to be gained from information technology will equate to a higher operational capability for the Interim Brigade Combat Team. The method of analysis will review the future operational environment for which this force is being developed, underscore the capabilities information technology brings to the transformation effort, and examine the challenges information technology presents Army planners and leaders as they further develop the campaign plan and execute the program. This study will suggest that accounting for the unintended consequences brought about by gains from information technology will contribute to a tighter fit between aspirations and emerging capabilities.

TABLE OF CONTENTS

ABSTRACT iii

LIST OF ILLUSTRATIONS vii

LIST OF TABLES ix

LEVERAGING INFORMATION TECHNOLOGY TO ENABLE ARMY TRANSFORMATION: CAPABILITIES AND CHALLENGES FOR THE INTERIM FORCE 1

INTERIM FORCE 2

FUTURE OPERATING ENVIRONMENT 5

INSTABILITY AND ASYMMETRIC THREATS 6

DOWNSIZING TO A POWER-PROJECTION ARMY 8

THE DECLINING BUDGET 10

CAPABILITIES GAINED FROM INFORMATION TECHNOLOGY 12

NETWORK CENTRIC WARFARE 13

OVERVIEW OF DIGITIZATION 15

KEY COMPONENTS 16

COMMUNICATIONS TRANSPORT 18

CHALLENGES FOR ARMY PLANNERS AND LEADERS 20

ACHIEVING NETWORK CENTRIC WARFARE CAPABILITIES 20

OVERCOMING UNANTICIPATED CONSEQUENCES AND COMPLEXITIES 21

OVERCOMING SYSTEM COMPLEXITIES 24

CONCLUSION AND RECOMMENDATIONS 26

ENDNOTES 31

LIST OF ACRONYMS 37

BIBLIOGRAPHY 41

LIST OF ILLUSTRATIONS

FIGURE 1. ARMY TRANSFORMATION CHART.....1

FIGURE 2. INTERIM BRIGADE COMBAT TEAM ORGANIZATIONAL CHART.....4

FIGURE 3. PLATFORM AND NETWORK CENTRIC WARFARE COMPARISON CHART.....13

LIST OF TABLES

TABLE 1. PEACE DIVIDEND AND THE ARMY 11

TABLE 2. ABCS HEIRARCHY 17

LEVERAGING INFORMATION TECHNOLOGY TO ENABLE ARMY TRANSFORMATION: CAPABILITIES AND CHALLENGES FOR THE INTERIM FORCE

> The nation demands an Army that is strategically responsive and dominant at every point on the spectrum of operations and capable of providing the National Command Authorities with a broad range of options for peacetime operations, deterrence, and warfighting.
>
> —Institute of Land Warfare,
> Association of the United States Army (AUSA)

The Army is on a rapid pace to transform itself to meet the new threats and challenges of the 21st Century. The new strategic vision, articulated in 1999 by the new Chief of Staff, General Eric K. Shinseki, calls for transforming the Army toward an Objective Force that is more responsive, deployable, agile, versatile, lethal, survivable, and sustainable.[1]

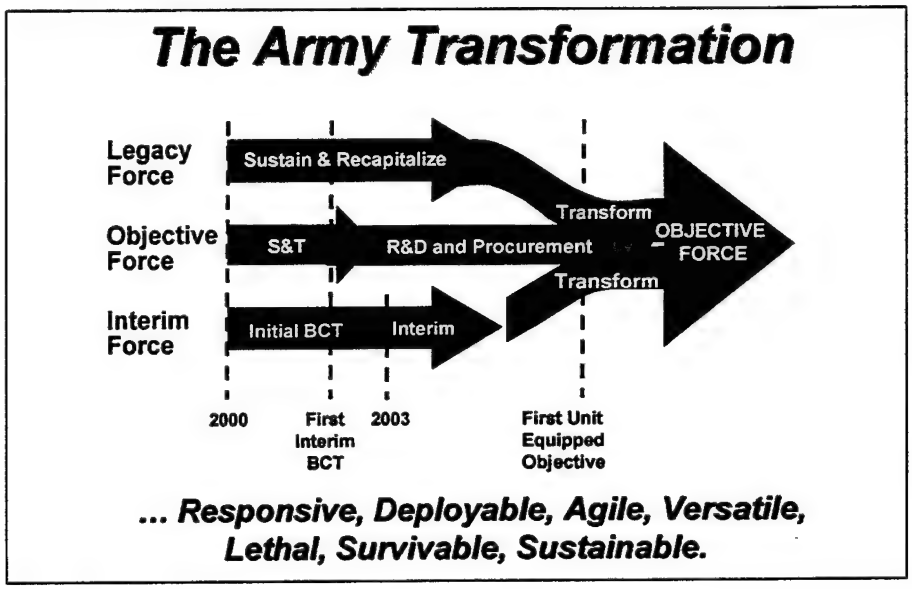


FIGURE 1: ARMY TRANSFORMATION CHART

Source: Department of the Army

According to the plan, which is graphically summarized in Figure One, the transformation effort will provide the National Command Authority (NCA) with a recapitalized Legacy Force to guarantee critical warfighting readiness, an Interim Force that will fill the strategic near-term capability gap that exists today, and a future Objective Force that achieves the Army Transformation objective with an increased range of options for regional engagement, crisis

response, and sustained land force operations.[2] The transformed Objective Force will achieve the seven force characteristics presented above (responsiveness, deployable, agile, versatile, lethal, survivable, and sustainable) that serve to describe and define the necessary capabilities.[3]

Two important events occurred over the last decade to cause the Army to begin the transformation process. The first event was the fall of the Berlin Wall and the end of the Cold War that changed the operational environment. This event significantly changed the political, military, and economic landscape of the world and lifted political and electronic barriers as well. When the wall came down, free enterprise took hold and telecommunications companies spread rapidly into areas where they were never before allowed. Thanks to microchips, satellites, fiber optics, the Internet, and reduced telecommunications costs, electronic barriers that existed during the Cold War were virtually eliminated throughout Europe and greatly diminished in Asia. Nations and corporations could speed the delivery of information to a point that erased time delays and expedited decision making processes. The second event that contributed to the Army transformation process was the Gulf War. The Gulf War was a vivid debut of precision munitions, instantaneous communications, satellite-aided navigation for ground troops, and new sensor technology, to name a few, that could display the enemy order of battle. As a result, the war demonstrated to the Army, the value of applying information technology to force development, doctrine, and organizational structure.

The purpose of this study is to examine the Interim Force and determine whether or not the anticipated higher technical performance gained from information technology will equate to a higher operational capability for the Interim Brigade Combat Team. The method of analysis will review the future operational environment for which this force is being developed, underscore the capabilities information technology brings to the transformation effort, and examine the challenges information technology presents Army planners and leaders as they further develop the campaign plan and execute the program. Lastly, it will present recommendations on how to mitigate the challenges in order to better realize the new operational capability. This study will suggest that accounting for the unintended consequences brought about by gains from information technology will contribute to a tighter fit between aspirations and emerging capabilities.

INTERIM FORCE

According to the Army's Transformation Campaign Plan, the Interim Force, "is a transition force that fills the strategic near-term capability gap that exists today—one that seeks the Objective Force to the maximum extent feasible, but leverages today's state of the art

technology together with modernized legacy forces to bridge a gap to the future."[4] The Interim Force, also known as the Interim Brigade Combat Team (IBCT), is full spectrum capable, medium in size and provides some distinct advantages for deployment in Small-Scale Contingency (SSC) operations and significant contributions in Major Theater of War (MTW) scenarios. According to the United States Army Transformation Campaign Plan synchronization estimates, the First Unit Equipped (FUE) is scheduled for March 01, the Initial Operational Capability (IOC) by December 01, and all IBCTs fully fielded by January 08.[5]

The Brigade Combat Team Organizational and Operational Concept document provides a doctrinal mission statement for the Brigade Combat Team:

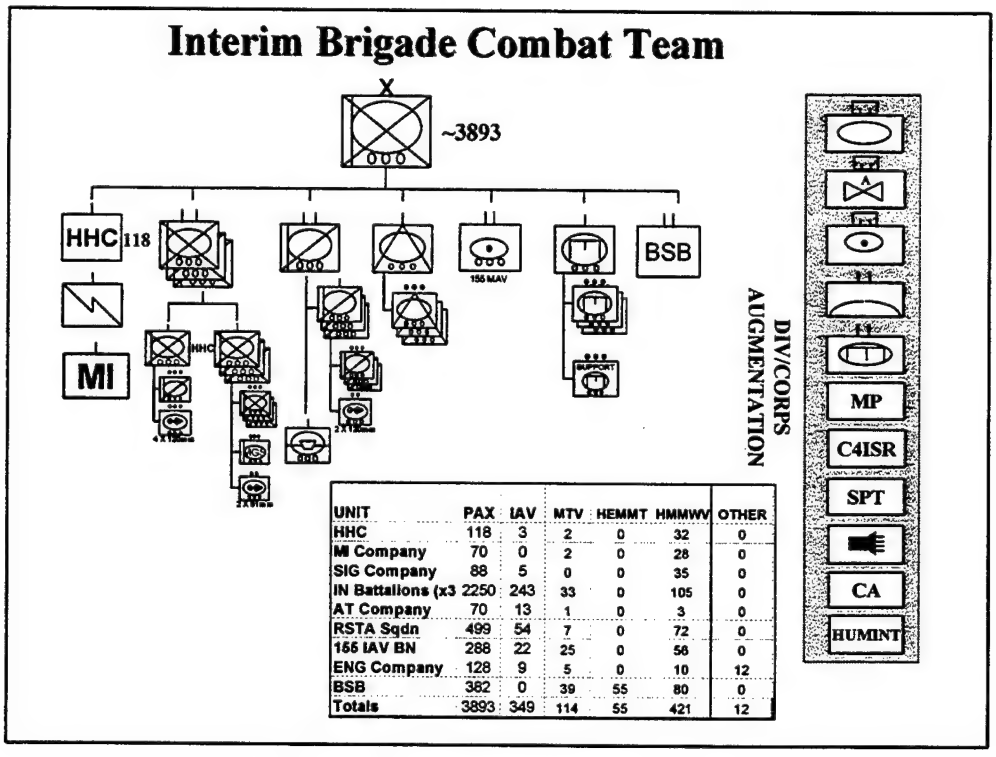
> The Brigade Combat Team (BCT) is a full spectrum combat force, designed primarily for employment in small-scale contingencies (SSC) in complex and urban terrain to meet low to mid-range threats that may employ both conventional and asymmetric capabilities. The BCT deploys rapidly to conduct combat operations immediately upon arrival to prevent, contain, stabilize, or resolve a conflict through shaping and decisive operations. The BCT participates in major theater war (MTW), with augmentation, as a subordinate maneuver component within a division or corps, in a variety of possible roles.[6]

This doctrinal mission statement provides some keen insight into what the Army's transformation plan is all about. As the key component, the BCT is intended to be full spectrum, able to operate independently, more suited to meet asymmetric threats, is rapidly deployable, and able to operate within a larger operational context, i.e. within a joint task force (JTF), Army Forces Headquarters (ARFOR), or coalition headquarters. In contrast to how a current brigade task force is organized for a particular mission, the BCT is a standing organization with its own embedded combat support (CS) and combat service support (CSS) organizations. Signal, intelligence, engineer, artillery, and CSS elements are uniquely tailored to support the BCTs mission set. The support elements are organized with common motorized vehicles, generators, and equipment to reduce sustainment and maintenance requirements and provide an overall smaller footprint in the operational area. The BCTs standing organization establishes a true foundation for consistent training relationships, and presents the opportunity for constant improvements in tactics, techniques, and procedures (TTP).

Concurrently with the embedded unit-based capabilities, the BCT offers a new organization called the Reconnaissance, Surveillance, and Target Acquisition (RSTA) Squadron to enhance situational understanding.[7] In practice, this organization would do what a normal cavalry squadron would do except it will use digital and networked computer technology to provide a situational awareness picture of the operational area. The situational awareness picture will include friendly and enemy locations, chemical early warning, and airborne

surveillance, to ultimately provide situational understanding for unit commanders. The RSTA squadron incorporates unmanned aerial vehicles (UAV), rotary wing reconnaissance assets, chemical units, and ground sensor elements as part of its organization. It has the ability to exploit the networking capabilities afforded by digitization to fulfill the vision of Network Centric Warfare (NCW) a term that captures the concept of information enabled military strategy. NCW has significant implications for the Army's transformation effort. It will be discussed in further detail in a subsequent section.

In addition to the RSTA Squadron as a new organization, the BCT will provide a more deliberate attempt to focus on Military Operations in Urban Terrain (MOUT). Using specific TTPs developed during the MOUT Advanced Concept Technologies Demonstrations (ACTD) at Fort Benning, Georgia, which included Close Quarter Marksmanship (CQM) and Close Quarter Combat (CQB) drills, Land Warrior technology developed for MOUT operations including heads-up display devices on the integrated helmet assembly subsystem, and wheeled armored vehicles to navigate city streets, the BCT will provide the precision necessary to fight and win in the urban environment.[8]



UNIT	PAX	IAV	MTV	HEMMT	HMMWV	OTHER
HHC	118	3	2	0	32	0
MI Company	70	0	2	0	28	0
SIG Company	88	5	0	0	35	0
IN Battalions (x3	2250	243	33	0	105	0
AT Company	70	13	1	0	3	0
RSTA Sqdn	499	54	7	0	72	0
155 IAV BN	288	22	25	0	56	0
ENG Company	128	9	5	0	10	12
BSB	382	0	39	55	80	0
Totals	3893	349	114	55	421	12

FIGURE 2: IBCT ORGANIZATIONAL CHART

Source: The Brigade Combat Team Organizational and Operational Concept Document, TRADOC, 22 February 2000

From an organizational standpoint, the IBCT does have some shortfalls. The IBCT is organized without organic aviation, air defense artillery, cannon artillery, combat and construction engineers, and military police. These organizations, according to the organizational and operational plan, will come from divisional augmentation packages tailored for the mission. This is quite different from what is normally provided to a brigade combat team that deploys to a national training center. Careful consideration will have to be given to this shortfall during preparatory activities and pre-mission planning in order to ensure the brigade has all the tools it needs to accomplish its mission. Even with these shortcomings, the IBCT will establish the foundation from which the Objective Force can improve upon as TTPs and SOPs are tested and doctrine is developed. This new organization is viewed in its larger IBCT context in Figure Two.

In theory, the BCT with its technological advancements, combined arms organization, and NCW capability, can provide national decision makers with a more efficient warfighting element that can operate across the entire spectrum of operations. The BCT would provide a wide range of capabilities for the NCA in its deployment, and for the Commander-in-Chief (CINC) or Joint Task Force (JTF) Commander in its employment. Regardless of the mission, the BCT is prepared to operate within the full spectrum of operations and with a joint, combined, or multinational headquarters.

FUTURE OPERATING ENVIRONMENT

The world in which the new Interim and Objective Forces might fight has also vastly changed. "For the first time in history almost the entire world population lives in a global capitalist system with the aim of free movement of goods and services."[9] This process known as globalization has positive and negative consequences on the economic, cultural, political, and technological landscape of the world.[10] According to Thomas L. Friedman in his book The Lexus and the Olive Tree, "globalization is not just some economic fad or passing trend, it is an international system that replaced the Cold War system after the fall of the Berlin Wall."[11] He defines globalization "as the inexorable integration of markets, nation-states and technologies to a degree never witnessed before—in a way that is enabling individuals, corporations, and nation-states to reach around the world farther, faster, deeper, and cheaper than ever before, and in a way that is enabling the world to reach into individuals, corporations, and nation-states farther, faster, deeper, cheaper than ever before."[12] The defining technologies of globalization include: computerization, miniaturization, digitization, satellite communications, fiber optics, and the Internet.[13] These new information technologies are weaving the world together, expanding

the global market place, creating jobs worldwide, and extending cooperation among allies and emerging democracies more than ever before.

The economy of the United States continues to thrive through this globalization era with its European, Asian, and middle-eastern partners. Free market economies have broken down historic barriers to free enterprise. Even Russia and former members of the Warsaw Pact now cooperate with the United States on numerous economic and political issues. The globalization phenomenon has had a leveling effect on the international economic, political, and technological playing field, providing many states with unparalleled access to defense and commercial technologies. The information revolution that flowered in the late 1980s made it possible for so many people to act globally, communicate globally, travel globally, and sell globally.[14]

Globalization has significant security implications. Despite the far-reaching impact of globalization on economies around the world, it has produced a powerful backlash from those brutalized or left behind by this new system. This backlash became evident during the first World Social Forum held in Porto Allegre, Brazil in January 2001. Organizers of this Forum attempted to embrace an alternate approach to globalization. "It was an effort to acknowledge the benefits of globalization while at the same time seeking ways to blunt its sometimes brutal impact on communities and labor forces."[15]

INSTABILITY AND ASYMMETRIC THREATS

The growing tendency of nation states to improve trade, economic, political, and technological ties with each other through globalization also has its problems. Potential adversaries have the same access to the global industrial base as the United States and other capitalist countries. Proliferation of technology, both military and civilian, is rampant around the world. Potential adversaries can easily obtain very sophisticated technologies that improve their traditional military capabilities or provide them new "asymmetrical" options. Given the explosion of communications, information accessibility, and technological proliferation, a wider range of actors are now in a position to influence world opinion and threaten our national security. No longer do we have a clear template of whom, where, or how an adversary can strike. Adversaries can attack our industrial, communications, financial, and political bases with relative ease using state-of-the-art technology that hides their location and identity. Given the technological edge the United States has in weaponry, the conventional military foe is becoming more reluctant to challenge the United States in traditional ways. Adversaries will look for ways to match their strengths against our weaknesses in a synergistic way to achieve political or

military goals. In the view of the Department of the Army, "The United States confronts a dynamic and uncertain international environment that poses complex challenges."[16]

A perfect example of what can happen in this uncertain environment occurred on 12 October 2000 at the port of Aden in the country of Yemen, when a terrorist team rammed a Zodiac boat filled with explosives into the port side of the USS Cole as it was refueling. Numerous sailors were killed and wounded as a result. As one security expert observed: "Twenty years ago it would have been difficult and more expensive to put together explosives that would blow a 40-by-40 foot hole in a modern destroyer. Today you can get this stuff by mail order."[17] Another example of uncertainty has been created by the abundance of weaponry to enter the foreign sales market since the break up of the old Soviet Union. Ammunition, small arms, equipment, and weapon systems have entered the market place at an alarming rate and are sold to state and non-state actors with little regard to the consequences. Even the conversion of military technology to the civilian sector can have repercussions. For example, "the $500 Global Positioning System that Hertz puts into its new rental cars can be used by terrorists to pinpoint targets."[18] In this uncertain environment, every technological innovation and every trade barrier lifted can easily have a second or third order adversarial effect on the United States.

Amplified by globalization, the world has become a more dangerous place and asymmetric means have emerged as a more likely threat to our national security. The proliferation of weapons of mass destruction (WMD) in the chemical, biological, or nuclear application; cyber warfare through the remote use of the ubiquitous internet; terrorist attacks against foreign and domestic sites; the growing drug trade; and organized crime are unconventional or asymmetric methods an adversary may use to exploit our weaknesses. The asymmetric threat may attack our will to fight, deny access to our information based systems, exploit WMD technology, target fixed installations and massed formations to name a few.[19] To complicate matters, asymmetric means have no boundaries whether its north or south; east or west; state or from a non-state actor; all avenues are open. The threat is not clear, the normal conventional linear military formations the Army has historically prepared for have changed; there is no peer competitor and asymmetric means have emerged as a less risky method for an adversary to use against the United States.

Arguably the cyber threat is probably the most likely of the asymmetric means that a potential antagonist could use to threaten the United States. The term "cyber warfare" refers to "conflict in the digital realm consisting of remote attacks on critical information nodes, links, and databases to disrupt, exploit, disable, or deny service".[20] Joint Publication 3-13, refers to cyber

warfare as "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[21] Considering the United States is heavily reliant on automation assets, computers, networks, and the internet, etc., the network servers, data base archives, and command and control nodes for industry as well as national defense systems are lucrative targets for cyber warfare opponents. The government, industry, and the Army have become heavily reliant on information-based systems to enhance operations and streamline processes. The Army uses computers and networks in garrison and field environments to conduct command and control, logistics, and intelligence operations, making cyber warfare a very realistic threat. Without the proper defense mechanisms in place it would be very hard to prevent an intrusion or a complete shutdown of a national defense, government, or industry based computer network from happening.

Considering the adverse consequences of globalization on National Security and the asymmetric threat associated with the process, global friction will occur as cultures, religions, governments, and economies interact in a highly competitive global setting.[22] "New regional powers and transnational actors will emerge onto the global scene as today's driving forces of demographics, economics, and technology move developing states into global economic networks and alter the balance of power within regions."[23]

The Army transformation process cannot resolve all the paradoxes that globalization creates in security relations, but it must appreciate the implications for where conflict will likely erupt and the types of combat Army forces must be able to conduct. Viewing the changing geo-strategic environment from a landpower perspective, the Army has designed the Interim and Objective Forces to be more suitable capabilities by making them lighter, more deployable, and better able to work within an information rich command and control context. Some of these changes have responded to the evolving security environment as just discussed, but others were the result of reductions in the size of the Army and changes in its worldwide disposition.

DOWNSIZING TO A POWER PROJECTION ARMY

In addition to the emerging asymmetric threat and proliferation of modern technologies through globalization, the strategic environment has changed domestically in the way the United States military has shaped itself over the past 10 years. Using the Army as an example, since 1989 the Army reduced its active forces by 275,000 shrinking from a 5 corps 18-division active duty force to a 4 corps 10-division present day active force.[24] To put this in better perspective, 21 active combat brigades were cut between 1989 and 2001 (53 to 32 respectively or a 40% reduction), and 277 active battalions were cut between 1989 and 2001 (778 to 551 respectively

or a 30% reduction).[25] In addition to the active force, the Army Reserve downsized 36% and the National Guard 23% from FY 89-01.[26] Oddly enough, while this massive downsizing effort was underway, Army deployments increased by 150%. Deployments went from 10 between 1950 and 1990 to 25 deployments from 1990 to present. This drastic downsizing effort combined with growing mission requirements has caused the Army to change from a forward-stationed Army to a power-projection Army.[27]

The power-projection concept depends on the ability to launch a sizable force from multiple bases throughout the Continental United States (CONUS) to distant corners of the globe. The Army's idealized concept of power projection has been described as follows:

> 1) A force with a full range of capabilities, able to deploy rapidly by land, air or sea. 2) Modernized Army installations that can enhance mobilization and deployment. 3) State-of-the-art, integrated information management to plan and monitor power projection. 4) Globally pre-positioned equipment and responsive war reserve support.[28]

Examples of power-projection platforms include: Fort Bragg, NC and adjacent Pope Air Force Base, Fort Drum, NY and Wheeler Sack Army Airfield, and Fort Stewart, GA and Hunter Army Airfield to name a few. According to the Secretary of Defense's Annual Report to the President and Congress for 2000, "effective and efficient global power projection is the key to the flexibility demanded of U.S. forces and ultimately provides national leaders with more options in responding to potential crises and conflicts."[29]

The migration to a power-projection Army from a forward-based Army has its disadvantages. One of which is the heavy reliance on airlift needed to get to the contingency area. The Air Force has a limited number of lift aircraft. "By the end of FY 2001, the military airlift fleet will consist of 58 C-17s, 88 C-141s, 104 C-5s, and 418 C-130s."[30] It usually takes a combination of these aircraft and a large number of sorties to conduct lift missions for any sizeable force. For obvious reasons, it's a lot easier to lift a light division or airborne division than it is to lift a heavy division equipped with M1 series Abrams main battle tanks, M2/M3 Bradley fighting vehicles, the Paladin field artillery system, or the Apache attack helicopters. Consequently heavy and light units have significantly different airlift requirements and response times.

By 2004, the Air Force expects to have 120 C-17 transport aircraft in their airlift force.[31] This total is far short of the number required to meet the airlift capacity of 54.5 million ton-miles per day to fight the two Major Theater of War (MTW) strategy as outlined in the "Mobility Requirements Study 2005" completed on January 10, 2001.[32] As impressive as the C-17 may be, it is also expected that further changes to the airlift fleet will be required if the Army is to

realize its vision of deploying an IBCT in 96 hours.[33] An important factor in Army Transformation success is clearly the synchronization of Air Force airlift procurement in the year 2004 and beyond.

In an effort to make power-projection more viable, the Army has tried to reduce airlift demand and improve response times by prepositioning equipment and supplies near potential conflict regions. Pre-positioned assets are stored afloat as well as on land and are strategically located to meet potential requirements. Locations include Southwest Asia (Kuwait, Qatar, Bahrain), Europe (Belgium, Italy, Norway), Pacific (Korea, Japan), and afloat in the Indian and Pacific Oceans.[34] Pre-positioned stocks are configured in brigade and Combat Service Support (CSS) sets, sustainment stocks and medical equipment, and are in adequate quantities to reduce the air and shipload requirements of deploying units. Without these pre-positioned stocks, it would be very difficult for the Army to meet any of the Major Theater of War (MTW) deployment timelines.

In addition to prepositioning, the Army has addressed this deployability requirement in its Transformation Campaign Plan. "The Interim Force units will be highly mobile at the strategic, operational and tactical levels. They will be C-130-like transportable and equipped with a family of Interim Armored Vehicles (IAVs), lightweight artillery and other available technology designed to ensure maximum lethality and survivability while increasing tactical, operational, and strategic maneuver."[35] Deployability is a core quality of the Interim Force. It is an essential capability for the Army in meeting its strategic responsiveness requirement and a key element in the Army's Transformation Campaign Plan.

THE DECLINING BUDGET

The declining Army budget also presents a challenge to Army planners as they try to fund Army Transformation. The Army budget has been in a constant state of decline in relative dollars since FY 89. "Since 1989, the Army has provided over 60 percent of the forces for 32 of 36 major deployments while at the same time its end strength was reduced by 33 percent and its infrastructure by 21 percent."[36] Meanwhile, the Army budget over this period of time declined from 14.5 billion in FY89 to 9.3 billion in FY01. The effects of the declining budget along with the increase in operating tempo (OPTEMPO), has had a telling effect on the Army. The Army has continued to spend its money on operations and maintenance (O&M) costs associated with the long list of peacekeeping deployments to such areas as Kosovo, Bosnia, Haiti, and Somalia and on its aging equipment that was procured largely in the 1970s and 1980s. During the Senate Armed Services Committee (SASC) hearing 27 September 2000, General Shinseki, the

Chief of Staff of the Army, highlighted in his conclusion that the Army has mortgaged future readiness to meet near term mission requirements.[37] General Shinseki's theme was echoed by General Henry Shelton, the Chairman of the Joint Chiefs of Staff, who characterized the problem as taking a "procurement holiday" to pay down the national debt as a result of the end of the Cold War.[38] The high OPTEMPO rate has caused a significantly greater wear and tear on equipment. In order to pay the Operations and Maintenance (O&M) costs, the Army has had to transfer funds from procurement, base operations, and research and development accounts to pay the bills. Table One represents how the peace dividend has affected the Army since FY 1990.

	FY 1990	*FY 2000*	*% REDUCTION*
Active/Reserve Division	18/10	10/8	36%
Active Reserve Sep Brigades	8/27	3/18	40%
Total Active Manpower	750,000	480,000	36%
Total Army Budget	$102.5 billion	$71.5 billion	30%
O&M	$35.9 billion	$24.65 billion	32%
Personnel	$42.7 billion	$28.6 billion	33%
Procurement	$16.87 billion	$10.55 billion	38%
RDT&E	$6.47 billion	$5.36 billion	17%

TABLE 1: PEACE DIVIDEND AND THE ARMY

Source: ARMY REPORT: Research and Development: Enabling Transformation (AUSA) Oct 2000

In November 1999, the Center for Strategic and International Studies (CSIS) published a study entitled Averting the Defense Train Wreck in the New Millennium by Daniel Gouré and Jeffrey M. Ranney. In the "train wreck" study, the authors contend that for the past decade, the American people have enjoyed a substantial peace dividend in the form of reduced defense spending.[39] This reduction in defense spending has adversely affected the modernization and procurement accounts of all the services. Equipment is aging at a rapid pace with no money set aside for the future. According to the study, 25 years has passed since the start of the most recent DoD procurement modernization cycle.[40] "The inescapable fact is that, in terms of maintaining and sustaining the military capabilities of the QDR (Quadrennial Defense Review) force—the desired force for FY 1997-2015—DoD is facing budget shortfalls of at least $100 billion per year instead of the range of $5-$25 Billion per year.[41] The Army's portion of the budget deficit lies between $20-25 billion of the total DoD shortfall. A more conservative

estimate was provided by the Congressional Budget Office study, stating that DoD needs $50 billion per year more to properly fund the QDR force.[42]

It is significant that both the CSIS study and the CBO estimate concluded that the DoD has been under funded significantly over the last decade. As a consequence, it will take a concerted effort by the Bush administration and congress to either fully fund the shortfall or develop a strategy that matches the deployment and OPTEMPO with the proper size force. At this point in the tenure of the Bush administration, it is not at all clear that a commitment to an expensive transformation effort will be given without significant reservations. This leaves the Army with a very challenging dilemma: how to transform itself on three axes of modernization (Interim Force, Legacy Force, and the Objective Force), in a highly constrained budgetary environment. The Army's ability to overcome the budget deficit will play a critical role in transformation's future.

In summary, the future operating environment for the Army has changed significantly since the breakup of the Soviet Union, both in terms of a non-peer competitor and the adverse effects of globalization. When the Soviet threat went away, so did much of the Army's force structure and budget that was designed to counter it. In its place, Small Scale Contingencies (SSC) and asymmetric attacks emerged as more likely threats to our national security. At the same time, the Army went from a largely forward stationed Army to a CONUS based Army relying on power projection as the method to launch forces globally. This new requirement to launch rapidly from power projection platforms with more deployable and lethal forces inspired the Army's Transformation process.

The other factor that is believed to make a powerful contribution to landpower is information technology. As noted earlier, the IBCT is being configured to benefit from the contributions of advanced sensors and related systems. These contributions are often captured under the rubric of Network Centric Warfare. This term was briefly introduced earlier. Understanding NCW and the way that it has been captured in new Army battlefield visualization and command and control systems is vital to understanding both the potential strengths and liabilities of the transformation process and the landpower forces it produces. Consequently the Network Centric Warfare (NCW) concept and the Army's implementation of it will be considered in great detail in the next section.

CAPABILITIES GAINED FROM INFORMATION TECHNOLOGY

It has been argued that information technology has become the single most dominant influence on every aspect of American and global societies over the past 10-25 years. "The

driving force behind this transformation is the remarkable science of semiconductors, which has shifted the world's economy from an industrial to an information base in a little over a quarter of a century.[43] Information technology with wireless telephones, networked computers, the world wide web, electronic storage capacities, vast amounts of electronic media, television, radio, precision munitions, optics, imagery, sensors, and satellite technology, amounts to an acute change in the way of viewing business, industry, government, and warfare. The National Defense Panel in December 1997 stated, "The rapid rate of new and improved technologies (a new cycle about every 18 months) is a defining characteristic of this era of change and will have an indelible influence on new strategies, operational concepts, and tactics that our military employs."[44] In the view of a prominent retired Army intelligence officer: "This technological revolution has led the military to change its vision and doctrine in order to master NCW and achieve 'information superiority' as outlined in Joint Vision 2020."[45]

NETWORK CENTRIC WARFARE

NCW is distinguished from industrial age or "Platform-Centric Warfare" (PCW) that used hierarchical procedures and stove-piped systems as the norm.[46] NCW is a new way of thinking about warfare and the information infrastructure that supports and amplifies the generation of military power. The term NCW best describes how the Army will fight in the Information Age using the concepts of shared awareness and self-synchronization.[47] Figure Three contains a PCW and NCW comparison chart.

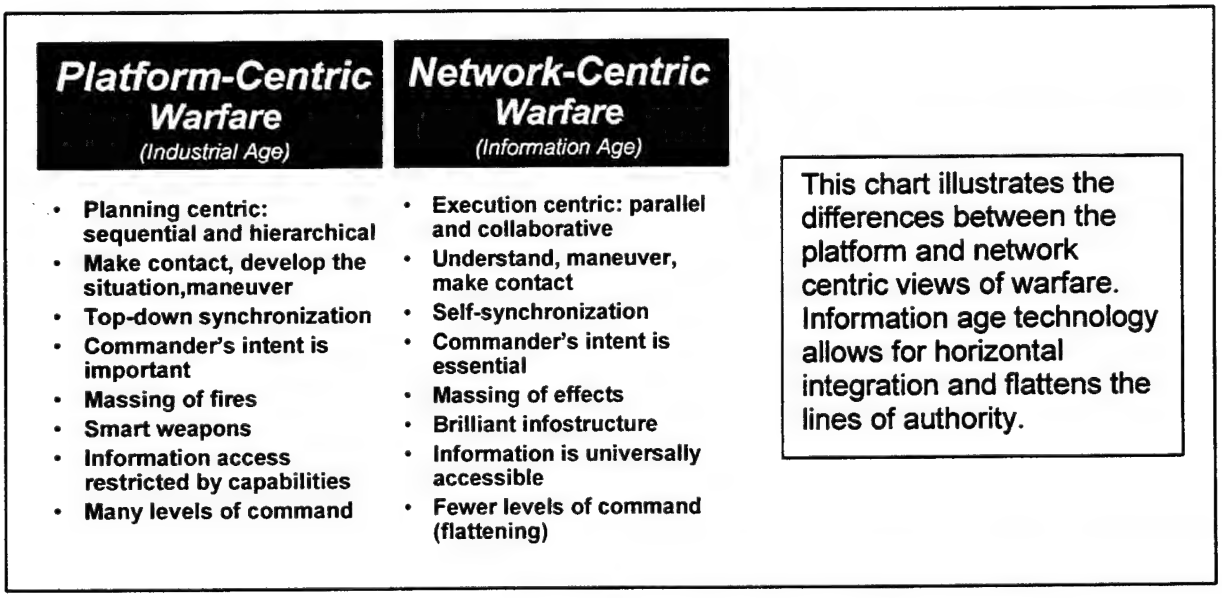


FIGURE 3: PLATFORM AND NETWORK CENTRIC WARFARE COMPARISON CHART

Source: Department of the Army

NCW is about learning to reap the benefits of networked computers and processors that are found in sensors, C2 systems, and weapons platforms to achieve synergistic effects. NCW capitalizes on the strengths found in these battlespace entities and frees up time for commanders to shape their battlefield environment rather than having them spend endless hours manually tracking blue and red force locations, or manually updating maps and operational graphics. NCW systems will provide a continuous feed of red force information from airborne surveillance, reconnaissance platforms, and satellite imagery systems as part of a sensor network that will input the Common Operational Picture (a term used to describe the unified view of the battlespace) to provide battlespace knowledge for commander's and staff at all levels. Blue force locations are updated constantly using GPS and the Enhanced Position Locating and Reporting System (EPLRS). The end result is a better-informed commander and staff that can concentrate on the operational art of war rather than the mechanics of gathering and updating data.

NCW best captures the essence of Information Superiority as outlined in Joint Vision 2020 and Joint Publication 3-13. Information Superiority is defined as: "the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying and adversary's ability to do the same."[48] In Joint Vision 2020, Information Superiority is the enabler for the operational concepts of Dominant Maneuver, Precision Engagement, Full Dimensional Protection, and Focused Logistics.[49] Information Superiority enables the joint force to attain Full Spectrum Dominance. NCW has been defined, as:

> An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increases survivability, and a degree of self synchronization.[50]

NCW is about exploiting all available information to maximize combat power. It's about focusing on the benefits of having sensors, deciders, and actors networked together to achieve synergistic effects during a military operation. NCW enhances battlespace awareness, provides a more timely flow of information, and reduces the decision making time to achieve a competitive advantage. NCW will help the Army generate and exploit Information Superiority to gain Full Spectrum Dominance. The Army's approach to NCW has been traditionally through a program called "digitization."[51]

OVERVIEW OF DIGITIZATION

Some Army units have already been "digitized" and have established digital networks to take advantage of commercial and industrial technology. Others, primarily because of money constraints, have remained analog or have been partially digitized. Digital networks are "networks in which the information is encoded as a series of ones and zeros rather than as a continuously varying wave—as in traditional analog networks."[52] Digital networks are interconnected computers and microprocessors that provide a continuous stream of data, voice, imagery, or message text from one hub or server or sub-system to another. According to the Office of the Director of Information Systems for Command, Control, Communication, and Computers (ODISC4) on the Army Staff:

> Digitization is the application of information technologies to acquire, exchange, and employ timely digital information throughout the battlespace, tailored to the needs of each decider (commander), shooter, and supporter—allowing each to maintain a clear and accurate vision of his battlespace necessary to support both planning and execution.[53]

The beneficiaries of digitization are maneuver, fires, signal, intelligence, logistics, aviation, and air defense artillery organizations operating as a combined arms team to accomplish a mission.

Networked computers are central to the digitization effort. The Army has invested heavily in computers, local area networks, and web and database servers, to automate and streamline functions in all aspects of Army organization from the tactical and strategic environment to garrison operations. Computers are everywhere and are used for just about every imaginable task. Navigation, digital switching at terrestrial and cellular telephone exchanges, high technology telecommunications centers, wheeled and tracked vehicle ignitions and internal wiring systems, communications equipment, aviation assets, personal computing, and the list is almost endless. The Army has capitalized on this computer age technology by networking computers to exchange voice, data, graphic, and video information. In digitizing its forces, the Army has taken advantage of what a digital signal offers over an analog signal. Digital signals are completely accurate and less subject to attenuation; they are the language of computers and are extremely fast compared to analog alternatives—mechanical teletypes, facsimiles, and magnetic tapes.[54] Networked computers have given the Army increased speed in processing information, greater capacity for storing and sharing information and data bases, enhanced flexibility in tailoring networks and command and control functions, greater access for local and remote users, and more types of messaging from casual email to record organizational traffic.

The IBCT will capitalize on the digitization effort by incorporating the key components of the Army Battle Command System (ABCS). The physical, procedural, organizational, and human dimensions of ABCS represent the epitome of Army digitization and of the services aspirations to fulfill the promise of NCW and Joint Vision 2020 information dominance. The substantial technical, engineering, and organizational complexity of the ABCS configuration has important implications for the capability of the IBCT, the larger Interim Force, and the Objective Force. Although complex, it is important to understand the technical details and interrelationships between the key components of the ABCS.

KEY COMPONENTS

The digitization concept is best described in the Army Battle Command System (ABCS) Capstone Requirements Document (CRD). ABCS is a system of systems (SoS) that are networked together to provide a particular ingredient to the common operating picture (COP) in Army Tactical Operations Centers (TOC) from corps through battalions.[55] ABCS battlefield automation systems consists of the Air and Missile Defense Planning and Control System (AMDPCS); Forward Area Air Defense Command and Control (FAADC2); Combat Service Support Control System (CSSCS); Advanced Field Artillery Tactical Data System (AFATDS); All Source Analysis System (ASAS); Integrated Meteorological System (IMETS); Digital Topographic Support System (DTSS); Force XXI Battle Command-Brigade and Below (FBCB2); Global Command and Control System-Army (GCCS-A); Integrated System Control (ISYSCON); Maneuver Control System (MCS); and the Tactical Airspace Integration System (TAIS).[56]

Of these ABCS systems, six are considered to be Acquisition Category One.[57] The six systems include MCS and FBCB2 for maneuver forces, ASAS for intelligence, AFATDS for fire support, FAADC2 for air defense, and CSSCS for logistics.[58] These Acquisition Category One (ACAT I) systems are essential for digital operations and will be fielded to the First Digitized Division (4th ID) and the IBCT.

ABCS is the key component to digitization from the standpoint of the warfighter and his staff. "ABCS will provide commanders, staff, and leaders, critical tactical, operational, and strategic (theater, national, and multinational) situational awareness information and automation management tools that are needed to respond to the rapidly changing situation in the area of operations."[59]

ABCS is an extension of the Defense Information infrastructure (DII), not a separate system, and is interoperable with other DoD systems through the protocols required in the Joint Technical Architecture (JTA).[60] It is interoperable with joint systems when the Army operates in

a joint or combined environment. ABCS is the enabler in the Army's ability to project the force, conduct decisive operations, shape the battlespace, and protect and sustain the force while achieving full spectrum dominance.[61] The battlefield automation systems along with their corresponding battlefield functional areas and communications transport mechanisms are depicted in Table Two.

BATTLEFIELD FUNCTIONAL AREAS (BFAs)	BATTLEFIELD OPERATING SYSTEMS (BAS)	BATTLEFIELD AUTOMATION SYSTEMS (BAS)	COMMUNICATIONS SYSTEMS
AIR DEFENSE	AIR DEFENSE	AMDPCS FAADC2	WIN TACTICAL SATELLITE COMMUNICATIONS SYSTEMS TACTICAL RADIO COMMUNICATIONS SYSTEM DMS
COMBAT SERVICE SUPPORT	COMBAT SERVICE SUPPORT	CSSCS	
FIRE SUPPORT	FIRE SUPPORT	AFATDS	
INTELLIGENCE AND ELECTRONIC WARFARE	INTELLIGENCE	ASAS IMETS	
MANEUVER	MANEUVER, C2, MOBILITY/COUNTER-MOBILITY SURVIVABILITY	DTSS, FBCB2, GCCS-A, ISYSCON, MCS, TAIS	

TABLE 2: ABCS HEIRARCHY

Source: ABCS CRD, TRADOC Program Integration Office Army Battle Command System

The most significant aspect of the corps and IBCT digitization plan is the Tactical Internet (TI). The TI consists of two primary segments, the Upper TI and the Lower TI. The Upper TI provides the mechanisms for digital communications horizontally between brigades, vertically between brigades and divisions, and between TOCs at all echelons. The Upper TI consists of the communications transport systems that are provided by the signal battalion/company's mobile subscriber equipment network and its associated assemblages. The Upper TI also includes the ABCS systems that are located at the division, brigade, and battalion TOCs. Those staff sections that have functional control over their application provide the ABCS systems at those locations.

The Lower TI provides the digital communications capability for brigade and below elements not located at TOCs. Communications links for the Lower TI are provided through a combination of signal battalion/company and user owned and operated equipment. The Lower TI is characterized by the Force XXI Battle Command Brigade-and-Below (FBCB2) system as the primary C2 platform. The Lower TI is comprised of a wireless network that uses the Single-

Channel Ground-to-Air Radio System (SINCGARS) and the Enhanced Position Location Reporting System (EPLRS) radios combined with Internet Controller (INC) routers to pass information. The two segments of the TI are designed to provide seamless data transfer throughout the digitized battlefield.

COMMUNICATIONS TRANSPORT

For the IBCT, the Army will rely on the Area Common User Modernization Program (ACUS-MOD) to provide increased bandwidth and reliability to the Army's Legacy and Interim force. ACUS-MOD is the recapitalization and technical insertion plan to get the legacy Army in better shape for data communications and to provide some essential tools for the IBCT in realizing its full capability. The ACUS-MOD program is a result of the information transport demands coming from Army Warfighting Experimentations (AWEs) conducted at Fort Hood, Texas, and Fort Drum, New York. The ACUS-MOD plan is designed to increase data transport capacity and improve information assurance at the tactical and strategic levels over Mobile Subscriber Equipment (MSE) and Tri-Service Tactical (TRI-TAC) systems.[62] MSE and TRI-TAC will remain the information transport systems for ACUS-MOD until FY08 when the Warfighter Information Network-Tactical (WIN-T) is fully fielded. WIN-T is the communications transport system for the Objective Force. ACUS-MOD will immediately increase data capacity over MSE via the Tactical High Speed Data Network (THSDN); it will increase the strategic and tactical mobility of TRI-TAC by fielding a single shelter switch, and will replace all 5-ton vehicles with High Mobility Multipurpose Wheeled Vehicles (HMMWVs).

For the First Digitized Corps (III Corps at Fort Hood, Texas), the plan is to insert commercial Asynchronous Transfer Mode (ATM) switch technology to increase transport capacity, add commercial data routers (like CISCO brand), procure High Capacity Line-of-Sight (HCLOS) radios for increased throughput in terrestrial connectivity, add a Video Teleconferencing (VTC) interface capability, and provide Intrusion Detection Systems (IDS) for network security.[63] For the IBCT, ACUS-MOD will provide a Brigade Subscriber Node, Battlefield Video-teleconferencing (BVTC) capability, a Secure Wireless Local Area Network (SWLAN), and a Network Operations Center-Vehicle (NOC-V).[64]

The ACUS-MOD program will gradually upgrade the Legacy and Interim Force to meet current and future demands for bandwidth during the FY04-FY08 period. Current data bandwidth available over the standard MSE Tactical Packet Network (TPN) is 16 kilobits per second (kbps) from a node center switch to an extension node, and 64 kbps between node centers.[65] The ACUS-MOD program will upgrade each node center and extension switch with a

Tactical High Speed Data Network (THSDN) package that will upgrade the data capability at a small extension node (SEN) from 16 kbps to 512 kbps.[66] This is a 32-fold increase in data throughput at a brigade headquarters. This new capability will go a long way in providing the IBCT with a more robust and capable MSE network to support the ABCS and tactical Internet architecture it will employ.

In addition to the terrestrial enhancements, the army will field three satellite systems to the FDD and IBCT to overcome the inherent limitations of line-of-sight systems. The first satellite system is the Global Broadcast System (GBS). GBS is a joint Air Force-Army program intended to provide all service users with a one-way, high speed information flow of high volume multi-media information such as imagery, maps, weather, data, logistics, air tasking orders, and operational orders.[67] The second system is the Secure, Mobile, Anti-jam, Reliable, Tactical, Terminal (SMART-T). This system will use the new Milstar satellite constellation. This system provides low to medium data rate communications capability and will not be used to transport ABCS produced data. The third satellite communications system is the man-pack and vehicular mountable Spitfire radio. The Spitfire will primarily be used for voice command and control requirements that are beyond line-of-sight.

In summary, the Army's digitization initiative involves the application of information technologies to acquire, exchange, and employ timely information throughout the battlespace. It takes advantage of the revolutions in electronics and information technologies to make dramatic gains in all battlefield operating systems from individual soldier to corps headquarters. Advances made by the scientific and computer industry in miniaturization, computer networking, and lighter weight technology has aided the process. One key aspect of this reasoning is evidenced by the changing microprocessor in computer technology today. This concept is best stated by Andrew Koch in his Jane's Defense Weekly article "Joining the Force" where he states:

> While miniaturization, robotics and advanced propulsion technologies will enable the development of sophisticated individual combat systems, networking could give those systems the capability to truly revolutionize the way in which wars are fought.[68]

Digitization and its focal point system of systems called ABCS, combined with communications transport improvements, will provide commanders the ability to collect and analyze information, develop plans and orders, and monitor the tactical battlefield while simultaneously planning for future operations. Components of ABCS and the communications transport assets that will provide the necessary connectivity can be found throughout the brigade area of operations down to company level. The brigade and battalion TOCs will have MCS, AFATDS, FAADC2,

ASAS, and CSSCS. Company and platoon headquarters along with combat vehicles will have FBCB2, EPLRS, and SINCGARS. The signal company that provides the communications transport will have the MSE backbone routers and responsibility for planning and maintaining the EPLRS network.

CHALLENGES FOR ARMY PLANNERS AND LEADERS

The legacy Army that was built to counter the Soviet threat during the Cold War was based on analog and industrial age technology.[69] It was "Platform-Centric" using separate command and control processes for fires, air defense, strike, intelligence, and combat support systems.[70] It placed emphasis on deliberate planning, massing of forces, rigid doctrine and provided very little battlespace awareness. The objective was for massive formations of armor, artillery, air defense, and aviation elements to work synergistically in combined arms operations to defeat the Warsaw Pact. Each weapon system operated independently of each other tied together by terrestrial communications means for command and control. Situational awareness was provided by maps and overlays posted in tactical operations centers with friendly and enemy locations updated manually by watch officers. Orders and directives were published via typewriters and stand-alone computers and distributed by secure or non-secure voice combat net radio, teletype, facsimile, courier, or disseminated during meetings and conferences. Data communications were tenuous at best and based on analog technology operating at low data rates. This legacy Army still exists today, although in a somewhat modified state.

The changes encompassed in the move to a fully digital and integrated ABCS poses a tremendous challenge for the Army. Today the Army has one corps that is partially digitized, two brigade combat teams that are being digitized as part of the Interim Force, and the rest of the Army that is largely analog with some digital capability. Two major challenges must be overcome in order for the Army to realize the full digital potential; achieving network centric warfare capabilities and overcoming system complexities.

ACHIEVING NETWORK CENTRIC WARFARE CAPABILITIES

In 1994, the Army Warfighting Experiments conducted at Fort Hood by the 4th Infantry Division (MECH), quickly displayed the value of digitization to warfighters. The use of ABCS at brigade and division TOCs, FBCB2 and the tactical internet at brigade and below, the Enhanced Position Location System (EPLRS) and Global Positioning Systems (GPS) throughout the area of operations, presented commanders, leaders, and staff at all levels with an unprecedented situational awareness picture. Elements within the 4th ID were using computers and software to perform tasks that were normally done over secure voice radio, courier, facsimiles, and stand-

alone computers. The Division, Brigade, and Battalion Commanders' vision of the battlefield was immense compared to what was previously available. The Maneuver Control System (MCS), All Source Intelligence and Analysis System (ASAS), and FBCB2 to name a few, were delivering automatic updates of blue and red force locations as elements moved. The Military Decision Making Process (MDMP) was shortened drastically and streamlined into an automated process with whiteboards, computer graphics, and video teleconferencing. This virtual collaborative planning process provided immediate feedback of mission analysis and course of action development information to commanders and leaders at all levels. The speed of command increased proportionately with the time gained through the automated MDMP process. Additionally, combined arms synchronization became easier with ABCS and FBCB2 using interoperable software to create a COP at all echelons of command.

OVERCOMING UNANTICIPATED CONSEQUENCES AND COMPLEXITIES

As impressive as NCW and ABCS are expected to be, the question has been asked if such reliance on technology might actually impose unanticipated costs that become a serious liability. Theoretically, NCW sounds very innovative and far reaching, yet can this heavy reliance on technology really produce the kinds of results desired? Might it become the Army's "Achilles' Heel' ... [that] creates a potential vulnerability that may be exploited by adversaries or adversely affected by inherent systematic problems[?]"[71]

The potential liability has already become evident. This was demonstrated by a number of systemic problems that occurred in March 1997 during the Task Force XXI Advanced Warfighting Experiment (AWE) at the National Training Center (NTC). During this rotation and AWE, unexplainable system failures would occur in the MCS and FBCB2 displays that would cause staff officers, commanders, and leaders to wonder if the information displayed was current or outdated.[72] This problem could be attributed to a number of things and is certainly not insurmountable, but it does leave a certain amount of doubt as to whether the systems within ABCS - especially the lower tactical internet (FBCB2, EPLRs, SINCGARS, etc.) - can perform up to expectations when the situation requires it. Mark Mandelas also points out in his report: Organizational Structures to Exploit the Revolution in Military Affairs, that a Navy wargame, "Global 98", "revealed the vulnerability of ground or space based networks and huge information databases to attack or disruption."[73] These episodes certainly indicated how quickly commanders and staffs could lose confidence in the accuracy of technical displays when unanticipated problems arise.

Unanticipated problems and eroding confidence in the output of command and control systems could also pose a significant problem for the IBCT. For example, on 14 November 2000, the Program Executive Office for the C3S two star review reported that their unfinanced requirement category in the ACUS MOD program did not include a security firewall feature set, nor intrusion detection system software for the Tactical High Speed Data Net (THSDN) routers.[74] The THSDN routers provide the backbone data routers for the MSE network that is established to support communications within the IBCT. One of the real dangers posed by this situation is when the IBCT establishes its non-secure personnel and logistics network (using its CSSCS platform), to the Non-Secure Internet Protocol Router Net (NIPRNET), it becomes more vulnerable to outside virus, intrusion, or cyber attacks. In other words, the system does not have a fully funded information assurance capability built into it. The decision not to fund this feature was probably made on the basis of a risk assessment. The question remains whether that risk assessment is appropriate given the level of complexity in the collective system architecture.

This point is further amplified by David Alberts in his book: The Unintended Consequences of Information Age Technologies. Alberts points out that our reliance on high-tech systems has created a host of information-related vulnerabilities. "The ubiquitous nature of these technologies provides our potential adversaries with capabilities that help them understand how to attack our information assets and give them the tools to do so."[75] Reliance on a highly complex computer network with numerous input and output points introduces a critical vulnerability to a network centric force. A successful attack by an adversary on the central network (perhaps the information grid), of a network centric force, could produce irreparable damage in its ability to operate. Further compounding the issue is the fact that cyber attacks can be launched from anywhere in the world if entry to the system can be gained through the Internet or NIPRNET. Particularly absent in the proposed IBCT organizational structure is an element designed to address the cyber threat or information operations as a whole. To the casual observer, it would seem advantageous to have an organization that could at least perform the defensive aspect of information operations.[76]

Another problem with the IBCT and perhaps the most important in realizing its NCW capability, is the long-term consequences of having an Army with a mix of analog and digital forces. Currently, III Corps and the IBCTs are the focus of Army digitization efforts. III Corps becomes digitized by FY04 to include 3rd Armored Cavalry Regiment (3rd ACR), III Corps troops, 1st Cavalry Division (1st Cav) and 4th Infantry Division (4th ID).[77] That means two divisions and one corps out of the Army's ten division-four corps force structure will be fully digitized (not

counting the IBCTs), while the rest of the Army will remain analog. This will pose a problem when a digitized IBCT is employed in an operation and the follow-on division is mostly analog. The IBCT will have to default back to the lowest common denominator that unites them. This common system may end up being a secure LAN running Windows NT with NT workstations using Microsoft Office software, or it may be a secure telephone. According to the United States Army Research Institute for Behavioral and Social Sciences, "for the foreseeable future, the Army's inventory of vehicles, equipment, systems, and devices will contain a variety of capabilities ranging from completely digitized to completely manual."[78] For example, out of the total inventory of about 7000 Army tanks in the year 2015, only 1079 will be M1A2 and M1A2 System Enhancement Program (SEP) tanks, and by 2009, approximately 1600 out of 6500 Bradley Fighting Vehicles (BFV) will be the M2A3 digitized version."[79] The situational awareness and understanding tools that the IBCT will have on hand will most likely not be available to the analog forces and will prevent the IBCT from realizing its potential. Interoperability or lack there of becomes a key issue in IBCT employment.

Joseph Caneva, in his Naval War College report: Network-Centric Warfare: Implications For Applying the Principles of War, explains how network centric warfare can prevent an operational commander from achieving the principle of war "unity of command," when operating in a coalition task force.[80] He cites the Gulf War as an example of how the United States was able to conduct a high technology warfare campaign, while most of its allies had to resort to more industrial age techniques. "If network centric warfare is to be another quantum leap in the ability to conduct war—a true Revolution in Military Affairs—its adoption by the U.S. armed forces will broaden by several orders of magnitude the disparity in war fighting ability between the United States and its allies or potential coalition partners."[81] This technology gap that continues to grow between the United States and its allies will have the unintended consequence of forcing the United States to carry a heavier burden in future wars in order to make maximum use of its information age capabilities. The IBCT will be caught in the middle of this technology gap.

As the United States military continues to modernize at a rapid pace using state of the art technology, it continues to distance itself from its allies in warfighting capability. The IBCT will bring this widening gap to the forefront when it is employed. As the Army's "kick off team", the IBCT equipped with the latest digital equipment and C2 devices, will be prepared to conduct very sophisticated combined arms operations. Allied partners on the other hand, who have not made the necessary investments in technology and munitions, will continue to play a minor, less technical role behind the scenes, as a secondary or tertiary effort. Interoperability problems

between the IBCT and its allies will exacerbate to the point that the IBCT will be the main effort by virtue of its unique capability rather than by some political or national policy. The technology gap will act as a divider rather than a uniter in military operations.

OVERCOMING SYSTEM COMPLEXITIES

Another challenge that Army planners and leaders face as they establish the Interim Force is overcoming the unintended consequences of system complexities. The IBCT will have a mix of current digital systems and commercial-off-the-shelf (COTS) systems.[82] This combination of military standard and COTS systems with different protocols and technical specifications will increase the complexity of network management. COTS systems are designed for a fixed, stable, non-changing environment while military standard systems are designed for electronically dirty and mobile environments. The primary challenge lies in applying the internet protocols such as the commercial transmission control protocol/internet protocol (TCP/IP), hypertext transfer protocol (HTTP), and hypertext markup language (HTML), in a fluid tactical environment on systems that aren't designed for constant moves. According to the Digitized Force Systems Architecture version 3.0, there are over 13,000 IP addressable devices in a digitized division. This amounts to somewhere in the neighborhood of 1500-2000 IP addressable devices for one brigade combat team.[83] Compare this to an analog brigade that has about 200 IP addressable devices.[84] This is a significant challenge for network managers and system administrators who have the responsibility to ensure routers are programmed correctly, IP addresses are written correctly, cabling and equipment is protected from electromagnetic interference (EMI), and the network remains operational.

According to John Blaine, a recent battalion commander for the 124th Signal Battalion, 4th ID, "ABCS systems are interconnected with each other to allow for horizontal integration. This means each ABCS server is now dependent on the other for network efficiency."[85] This becomes a problem when one ABCS server drops out for some reason as it can cause some unintended effect on a totally unrelated system. He further states, "Isolating problems within this data network is becoming increasingly more complex, for these systems can fail in subtle ways."[86] He observed problems cascading throughout the ABCS network for reasons unknown to anyone, effectively masking the root cause. When running network diagnostic programs to try and pinpoint the fault, the diagnostics tended to compound and further mask the problem. Interestingly enough, there is no central network manager or system administrator to program, monitor, or troubleshoot what amounts to three different networks: the communications transport system, TOC ABCS systems, and the lower TI consisting of SINCGARS, EPLRS, and

FBCB2.[87] The signal battalion commander has direct control of about 14% of the networks' routers, while 86% of the routers reside in unit TOCs and combat vehicles.[88]

The phenomena that LTC Blain described was also observed by Larry Downes and Chunka Mui in their book: Unleashing the Killer App: Digital Strategies for Market Dominance. These authors characterize the second order effects of technology infusion as the "Law of Disruption."[89] The Law of Disruption is the second order effect of combining Moore's Law (every 18 months computer chip density increases while cost remains constant), with Metcalf's Law (that networks dramatically increase their value with each additional node or user). Simply stated it means: Social, political, and economic systems change incrementally, but technology changes exponentially.[90] The Law of Disruption can be applied to the Army as it transforms to the Interim Force. Technology change initially affects technology, but once critical mass is reached, the disruption takes place in other, unrelated systems. When the Army transforms to more sophisticated digital systems disruption occurs in unrelated systems like doctrine, training, material, and organization. The digitization of the IBCT and the move to network centric warfare capabilities creates a lagging gap between doctrine (how to fight digitally), training (new training requirements for leaders and soldiers emerge), material (acquiring the technology in a way that keeps up with industry, but does not further erode capability), and organization (how best to organize to reap the benefits of networking and digitization).

The human task of making all of these systems work together is a hugely complex issue that relies on the talent and training of the workforce. However, the IBCT will also face what the 4th ID currently experiences today; soldiers and officers who report to the unit untrained in digital skills. Currently there is no digitized warfighting doctrine, to include integration of systems, degraded operations, or mixed forces operations.[91] Soldiers with signal related specialties have received little or no training on the unique information technology equipment found in the 4th ID and certainly not at the networking level. "Networking is the glue that that pulls the disparaging systems together as a synergistic system. For the signal community, this is the single most critical training shortfall."[92]

Non-signal soldiers may have received training on their unique ABCS system, but are very unlikely to have received any training on all of the ABCS systems, or to have any idea of how the ABCS systems inter-relate to provide a common operating picture in a brigade or battalion TOC. "The amount of additional knowledge that commanders and their staffs must have to properly operate these systems and to understand the feedback that they provide adds to their knowledge burden."[93] The ABCS systems are so complex, that it has taken a slew of contractors and support personnel to install, operate, and maintain the individual systems. This

lack of technical training and over-reliance on contract support in using the ABCS systems puts a tremendous burden on the unit affected in realizing its operational potential.

With the proliferation of high tech systems in the brigade and battalion TOCs combined with high tech nodes spread throughout the brigade area of operations, increases the need for trained and qualified maintenance personnel. Based on experience, untrained maintenance technicians have a tendency to replace parts more often than those that are trained. The consequences of such actions can lead to costly removal of parts that are not malfunctioning, further delaying the systems operational status.[94] Most maintenance personnel are centrally located and rely on each other's expertise to solve complicated problems, (the theory of two heads are better than one). Some faults are so complicated that it takes the entire section to work the problem. When multiple problems occur on a dispersed battlefield, it becomes harder to mass technicians, and harder to send the right person to do the right job. When conducting high paced operations in a fluid environment made possible by networked ABCS systems, new types of maintenance and troubleshooting problems occur. The continuous cabling and re-cabling, packing and re-packing of automation equipment combined with improper shutdowns, data loss, data corruption, failed drives, software glitches and a host of other problems will surge to point where trouble calls will totally consume the waking hours of signaleers and maintenance technicians.

From its inception, unintended or not, the "network" appears to be the center of gravity in digital operations. Army leaders and planners face a challenging task in overcoming system complexities that are associated with using, operating, and employing complex digital equipment.

CONCLUSION AND RECOMMENDATIONS

The Army is on a rapid pace to transform itself to meet the new threats and challenges of the 21st century. The Interim Force is the first step toward the Army reaching its goal of having a more responsive, deployable, agile, versatile, lethal, survivable, and sustainable force. The Interim Force will be the foundation from which the Army builds on its transformation campaign plan. The tactics, techniques, procedures, and lessons learned that are developed and experienced by the first two IBCTs at Fort Lewis, Washington, will set the foundation for Army Transformation.

The Army will use information technology to enable its transformation effort. The systems and networking tools developed by industry and exploited through the AWE process in the mid-to-late 1990's at Fort Hood, Texas, will be used to outfit the Interim Force. The Army

expects to leverage this technology to advance the concept of digitization and network centric warfare, the concept of networking sensors, shooters and C2 systems digitally, to provide a clear and accurate vision of the battlespace. Network centric warfare will help the Interim Force generate and exploit information superiority to gain full spectrum dominance. In order to leverage information technology most effectively, the Army must overcome two major challenges: find a way to achieve network centric warfare capability and overcome the complexities of digital technology.

There are five sets of recommendations that the Army should consider in the development of the digital infrastructure supporting the IBCT. These are: active experimentation in the development of doctrine; planning for the analog-lag; protecting the network center of gravity; managing configuration complexity, and training the digital workforce.

ACTIVE EXPERIMENTATION

No system ever makes its debut without a host of bugs that must be worked out. A system of systems as complex as the ABCS infrastructure in the IBCT will have an extraordinary number of engineering, organizational, operational and doctrinal issues to resolve before it reaches full capability. The best way to overcome these challenges is to have a period of active experimentation when the Army can allow the IBCT to debug the systems and develop the initial doctrine of how to fight digitally through a trial and error process. The IBCT leaders can work with TRADOC and the 4th ID to capture the learning process and the innovative procedures that the IBCT creates to master the new sensor-shooter-C2 node architecture. The dynamic doctrine and operational guidance that comes out of the experimentation process can explain how to mass the effects of geographically dispersed shooters in a more responsive, accurate, and lethal manner. It should describe how the battlespace is shaped to maximize combat power and lock out enemy courses of action. Leaders can ensure this doctrine is linked to JV2020 so the military as a whole is speaking with one voice. The doctrine should be taught in the branch schools and the joint professional education program to properly educate leaders.

DEALING WITH THE ANALOG "LAG"

Another critical requirement for the doctrine is to address the complications involved in merging analog and digital forces. The Army will have a mix of digital and analog forces for the next 30 years. It is essential that tactics, techniques, and procedures are developed that allows each force to operate together and in a synergistic way to accomplish its mission. A supporting solution is to establish liaison teams outfitted with MCS boxes and communications transport systems and place them in the analog Army, joint organizations, or multi-national headquarters,

to provide the necessary resources and a common denominator that will allow key leaders to have the same common operational picture as the IBCT. This liaison team could consist of an operations, intelligence, and fire support officer/non-commissioned officer, with a communications team that links to the IBCT's backbone network via satellite radio or a terrestrial based system, depending on the terrain and unit locations. The objective of the liaison teams would be to provide the critical situational awareness picture and collaborative planning capability that the IBCT would possess. This would also solve any interoperability issue that might arise and would go a long way towards reducing the issues associated with classification of information and release authority.

The IBCT should also strive to temper its desire to rely totally on digital and automation systems for all its C2 needs. It would be prudent to maintain a backup analog capability for instances where analog forces are integrated with digital forces and an automated link cannot be established. Leaders can ensure their soldiers are trained in both skill levels to facilitate a continuity of effort in operations. The IBCT should train and prepare for catastrophic situations that commonly occur with networked systems and have a seamless transition to a manual backup. Unexplained outages, weather damage, generator failure or lack of fuel can play havoc with networked operations and totally disrupt any momentum gained by its use. Having an analog backup capability is essential to maintaining a viable fighting force.

PROTECTING THE NETWORK CENTER OF GRAVITY

In NCW operations, the "network" has emerged as the center of gravity to successful operations. It is therefore essential to protect the network from radio-electronic and cyber threats from outside sources. This is a systems engineering and a procedural problem. Every effort should be made to ensure that proper information assurance devices whether its firewalls, anti-intrusion/detection software, or anti-virus software, is procured in the right amounts to protect the network. Maximum use should be made of the anti-jam capability of SINCGARS radios and SMART-T satellite terminals to provide the safest transmission path for voice and data within the IBCT. Leaders must take great care in site selection for key C2 nodes and mask signals with the available terrain. Re-look the organizational structure of the IBCT and find a way to establish an information operations element to oversee all aspects of information operations. Curb the appetite of those who think more information and more NIPRNET gateways are better. Guard against information overload and if anything reduce the number of gateways. In a NCW organization, network security is paramount.

MANAGING CONFIGURATION COMPLEXITY

In order to overcome the system complexities associated with digital operations, the IBCT must invoke some organizational changes in the delegation of responsibilities as well as undertake some specific system configuration engineering management initiatives. The IBCT must have a central element charged with conducting network management and system administration duties. These two elements must operate in harmony to reduce the complexity of managing three independent sub-architectures (ABCS, transport network, and lower tactical internet). This new element can work with software developers to create a dynamic IP routing capability at all levels of the IBCT to facilitate rapid task organization changes that often occur in a fluid tactical environment. With over 1500 IP addressable devices potentially in an IBCT, manually distributing floppy disks to every vehicle to change a task organization is extremely time consuming and counter-productive.

The challenge for the ABCS software developers has been to design a software package that will allow for horizontal integration of ABCS systems. One that would allow changes in the COP to be reflected on all ABCS systems as it is updated on one system. Software glitches have prevented this from happening in past versions. It is incumbent upon the IBCT to ensure this occurs in future versions and that the dependency of one ABCS system on the performance of another is reduced in a manner that will ease the troubleshooting challenges that system administrators are faced with.

Inside the digital TOC, many problems with system performance and operational status depend on whether or not the cabling of computers are done correctly and whether communications wires are separated from power cables. One solution to this wiring headache would be to establish a secure wireless LAN capability inside the TOC as soon as possible. ACUS-MOD has a funding line for a secure wireless local area network (SWLAN) for TOCs, but under the current funding constraints may not be available for several more years. Efforts should be made to make this a priority for the TOC in order to reduce the complexities associated with cabling and re-cabling as the unit displaces.

TRAINING THE DIGITAL WORKFORCE

Like 4th ID, the IBCT will be faced with having to train its new personnel on digital operations and networking. In the past, technical training such as this, was a requirement for signal personnel, now the technical training requirement has passed on to the end user. Commanders and leaders must understand this paradigm shift. No longer are the combat arms soldiers and leaders just concerned with their warfighting task, they must now know how to

operate and maintain their C2 system. The IBCT leaders should establish training programs that address the technical training issue just as importantly as they train in warfighting skills. With the few signaleers and maintenance technicians available, it is the only way the IBCT will come close to realizing the benefits of digitization and NCW capabilities.

The transformation to the Interim Force will not happen overnight. If the right emphasis is placed on active experimentation, dealing with the analog lag, protecting the network center of gravity, managing configuration complexity, and training the digital workforce, the Interim Force capability will be realized. The Army must continue to leverage information age technology to enhance operations while at the same time maintaining a viable analog capability, as both are the keys to success in the Army's Transformation Campaign plan.

WORD COUNT = 11,585

ENDNOTES

[1] Eric K. Shinseki, The Army Vision (Washington, D.C.: U.S. Department of the Army, 1999), 3.

[2] Louis Caldera and Eric K. Shinseki, United States Army Transformation Campaign Plan (Washington, D.C.: Headquarters, Department of the Army, 27 October 2000), 6-7.

[3] Ibid., 7.

[4] Ibid., 9.

[5] Ibid., 9.

[6] U.S. Army, Training and Doctrine Command, Director, Combat Developments, "The Brigade Combat Team Organizational and Operational Concept" (Fort Monroe, VA: United States Army Training and Doctrine Command (TRADOC), 22 February 2000), 6-7.

[7] Ibid., 20.

[8] U.S. Army, Department of the Army, Weapon Systems (Washington, D.C.: U.S. Government Printing Office, 2000), 1. This publication describes in detail every Army program from the basis of six categories: project the force; protect the force; gain information dominance, shape the battlespace, conduct decisive operations, and sustain the force.

[9] Patrick Dixon, "Poor Nations React to Globalization," available from <http://www.globalchange.com/globalis.htm>; Internet; accessed 15 January 2001.

[10] William J. Clinton, A National Security Strategy For A New Century (Washington, D.C.: The White House, October 1999), 49.

[11] Thomas L. Friedman, The Lexus and the Olive Tree (New York, NY:, Anchor Books, April 2000), 7.

[12] Ibid., 9.

[13] Ibid., 9.

[14] Ibid., xix.

[15] Stephen Buckley, "Foes Take Moderate Tack on Globalization," Washington Post, (Washington, D.C.: Saturday, January 27, 2001), A15.

[16] U.S. Army, Department of the Army, Weapon Systems, 132.

[17] Fareed Zakaria, "The New Twilight Struggle," Newsweek, 23 October 2000, 37.

[18] Ibid.

[19] National Defense Panel, Transforming Defense, National Security in the 21st Century (Washington, D.C.: U.S. Government Printing Office, December 1997), 11.

[20] Ryan Henry and C. Edward Peartree, The Information Revolution and International Security (Washington D.C.: The CSIS Press, 1998), 118.

[21] Joint Publication 3-13, Joint Doctrine For Information Operations (Washington, D.C.: The Joint Chiefs of Staff, 9 October 1998), GL 7.

[22] U.S. Army, Training and Doctrine Command (TRADOC), "The Foundations of Army Transformation and the Objective Force Concept Final Draft" (Fort Monroe, VA: 16 December, 2000), 6.

[23] Ibid., 6.

[24] U.S. Army, Financial Management and Comptroller, The Army Budget, FY 01 President's Budget (Washington, D.C.: U.S. Department of the Army, 2000), 8. This document represents the Army's 2001 budget request as submitted to Congress on 7 February 2000.

[25] Ibid., 28.

[26] Ibid., 14.

[27] The Institute of Land Warfare, Profile of the Army, a Reference Handbook (Arlington, VA: Association of the United States Army, February 1997), 28.

[28] U.S. Army, Financial Management and Comptroller, The Army Budget, FY 01 President's Budget, 9.

[29] William S. Cohen, Annual Report to the President and the Congress (Washington, D.C.: Government Printing Office, 2000), 16.

[30] Ibid., 50.

[31] Simon Seena, "Pentagon Report Cites Sagging Airlift," Army Times, 29 January 2001.

[32] Ibid.

[33] Simon Seena, "Lighter, Faster Forces Depend on Success of Air Force Airlift Makeover," Army Times, 29 January 2001.

[34] The Institute of Land Warfare, Fiscal Year 2001, Army Budget and Analysis (Arlington, VA: Association of the United States Army, July 2000), 74.

[35] Caldera and Shinseki, United States Army Transformation Campaign Plan, 9.

[36] The Institute of Land Warfare, Fiscal Year 2001, Army budget Analysis, 38.

[37] U.S. Senate, Committee on Armed Services, Full Committee, Testimony on the Status of Military Readiness. 106th Congress, 2d sess., 27 September 2000.

[38] Ibid.

[39] Daniel Gouré and Jeffrey M. Ranney, Averting the Defense Train Wreck in the New Millennium (Washington, D.C.: The CSIS Press, November 1999), xiv. This book has gained a lot of notoriety over the past year for its critical look at defense spending during the Clinton administration.

[40] Ibid., xv.

[41] Ibid., 2.

[42] U.S. Congress, Congressional Budget Office, Budgeting for Defense: Maintaining Today's Forces, 106th Congress, 2d sess., September 2000.

[43] Larry Downes and Chunka Mui, Unleashing the Killer App: Digital Strategies for Market Dominance (Boston, MA: Harvard Business School Press, 2000), 5.

[44] National Defense Panel, 7-8. Moore's Law began as a prediction by Intel founder Gordon Moore thirty years ago. He predicted that every eighteen months computer chip processing power would double while cost remained constant.

[45] Wayne M. Hall, The Janus Paradox: The Army's Preparation for Conflicts of the 21st Century (Arlington, VA: The Institute of Land Warfare, Association of the United States Army, October 2000), 3.

[46] Arthur K. Cebrowski and John Garska, "Network Centric Warfare: Its Origin and Future," Naval Institute Proceedings, January 1998, available from <http://www.usni.org/Proceedings/Articles 98/Procebrowski.htm>; Internet, accessed 2 February 2001.

[47] David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority (Washington, D.C.: DoD C4ISR Cooperative Research Program, August 1999), 55.

[48] Joint Publication 3-13, I-10, I-11.

[49] Henry H. Shelton, Joint Vision 2020 (Washington, D.C.: The Joint Chiefs of Staff, June 2000), 8.

[50] David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2.

[51] U.S. Army, Directorate of Army Integration, Army Digitization Master Plan (Washington, D.C.: Headquarters, Department of the Army, 1996).

[52] Harry Newton, Newton's Telecom Dictionary (New York, NY: Miller Freeman, Inc., August 1999), 249.

[53] William H. Campbell, "Force XXI...What You Can Expect to See", briefing slides, Director of Information Systems for Command, Control, Communications, and Computers, Department of the Army, June 2000.

[54] David S. Alberts and Daniel S. Papp, The Information Age: An Anthology on Its Impacts and Consequences, Volume I, Part One: The Information and Communication Revolution (Washington, D.C.: National Defense University Press, 1997), 105.

[55] U.S. Army, Combined Arms Center, "Army Battle Command System Capstone Requirements Document Revision 1c", (Fort Leavenworth, KS: TRACOC Program Integration Office Army Battle Command System, 3 October 2000), 7.

[56] Ibid.

[57] ACAT I systems are those systems that have a Research, Development, Test, and Evaluation (RDTE) budget value greater than $355 million and a procurement value greater than $2.13 billion. U.S. Army, How the Army Runs: A Senior Leader Reference Handbook (Carlisle Barracks, PA: U.S. Army War College, 1999-2000), 11-10.

[58] General Accounting Office, Battlefield Automation: Performance Uncertainties Are Likely When Army Fields Its First Digitized Division (Washington, D.C.: U.S. General Accounting Office, July 1999), 12.

[59] GAO, Battlefield Automation: Performance Uncertainties Are Likely When Army Fields Its First Digitized Division, 22.

[60] U.S. Army, Director of Command, Control, Communications, and Computers (ODISC4), Joint Technical Architecture-Army Version 5.5 (Washington, D.C.: Department of the Army, 23 December 1998).

[61] William H. Campbell, "DISC4 Overview Briefing to Mr. Dahlberg," briefing slides, Director of Information Systems for Command, Control, Communications, and Computers, no date.

[62] Anthony D. Tabler and Thomas Nugent, "Project Manager Warfighter Information Network-Terrestrial Two Star Review," briefing slides, Fort Gordon, U.S. Army Signal Center, 14 November 2000, 5.

[63] Ibid.

[64] Ibid.

[65] U.S. Army, FM 11-43, The Signal Leader's Guide (Washington, D.C.: Department of the Army, 12 June 1995), 3-45.

[66] Brian Hamilton and Walton Brown, "Tactical High-Speed Data Network: The Interim Army's Answer to Battlefield Data Transport," available from <http://www.gordon.army.mil/regtmktg/AC/SPR00/thsdn.htm>; Internet: accessed 25 January 2001.

[67] GAO, Battlefield Automation: Performance Uncertainties Are Likely When Army Fields Its First Division, 7.

[68] Koch, Andrew, "Joining the Force," Jane's Defence Weekly, 25 October 2000, 24.

[69] Douglas A. Macgregor, Breaking the Phalanx: A New Design for Landpower in the 21st Century (Westport, CT:, Praegor Publishers in cooperation with the Center For Strategic and International Studies, 1997), 59-60.

[70] Mark D. Mandelas, Organizational Structures to Exploit the Revolution in Military Affairs, (Fairfax County, VA:, January 2000), 47.

[71] Major Daniel Roper observes: "With Force XXI being heavily dependent on integration of technological advances into Army systems and processes, its Achilles' Heel may be over reliance on technology." Daniel Roper, "Technology: Achilles' Heel or Strategic Vision?" Military Review, March-April 1997; available from <http://www-cgsc.army.mil/milrev/milrvweb/html>; Internet; accessed 25 January 2001.

[72] Jack D. Flowers, Digitization of the Heavy Maneuver Brigade: Increased Situational Awareness and Decreased Decision Making, 1998: available from <https://calldbpub.leavenworth.army.mil/>; Internet; accessed 1 February 2001.

[73] Mandelas, 47.

[74] Anthony D. Tabler and Thomas Nugent, "Project Manager Warfighter Information Network-Terrestrial Two Star Review," briefing slides, 14.

[75] David S. Alberts, The Unintended Consequences of Information Age Technologies, April 1996,available from <http://www.dodccrp.org/ucHome.htm>; Internet; accessed 5 February 2001.

[76] Joint Staff Brochure, Information Warfare: A Strategy for Peace...The Decisive Edge in War, (Washington, D.C.: The Joint Chiefs of Staff), 7-8.

[77] U.S. Army, Digitization Office, Report on the Plan for Fielding the First Digitized Division and First Digitized Corps, Presented to The Committee On Armed Services, United States Senate, Second Session, 106th Congress, (Washington, D.C: Department of the Army, April 2000), 13.

[78] Roy Campbell, Laura Ford, Michael Shaler, and Robert Cobb, Issues and Recommendations: Training the Digital Force, (Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, August 1998), 3.

[79] Ibid., 3. Also, the International Institute for Strategic Studies (IISS) in their book: The Military Balance 1999-2000, report that the United States Army has 7,684 main battle tanks: 40 M60A3, 7,644 M1 variants (M-1A1, M-1A1A2). They also report 6,715 M-2/M-3 Bradley's and 17,800 M-113A2/A3 variants, see page 21. These numbers represent the total Army.

[80] Joseph W. Caneva, Network-Centric Warfare: Implications For Applying the Principles of War (Newport, R.I.: Naval War College, 17 May 1999), 10.

[81] Ibid.,10.

[82] Roy Campbell and others, Issues and Recommendations: Training the Digital Force, 6.

[83] U.S. Army, Office of the Director, Information Systems for Command, Control, Communications, and Computers, Digitized Force Systems Architectures: Blueprints for a Force XXI Army, CD-ROM v3.0 (Washington, D.C.: Department of the Army, 30 March 2000).

[84] Randall G. Conway, "Leader's MSE Handbook," and professional notes (Fort Drum, NY: 10th Signal Battalion).

[85] John M. Blaine, First Digitized Division: The Challenges in Realizing the Tactical Internet, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 10 April 2000), 7.

[86] Ibid., 9.

[87] John M. Blaine, "First Digitized Division Challenges," briefing slides with notes, Office of the Director for Command, control, Communications, and Computers, Department of the Army, February 2000, 24.

[88] Blaine, First Digitized Division: The Challenges in Realizing the Tactical Internet, 9.

[89] Larry Downs and Chuka Mui, Unleashing the Killer App, 29.

[90] Ibid., 29. Metcalf's Law refers to Robert Metcalf, founder of 3COM Corporation and the designer of the robust Ethernet protocol for computer networks, observed that new technologies are valuable only if many people use them. Specifically, the usefulness, or utility, of a network equals the square of the number of users, a function known as Metcalf's Law.

[91] Campbell, Issues and Recommendations: Training the Digital Force, 9.

[92] Blaine, First Digitized Division: The Challenges in Realizing the Tactical Internet, 13.

[93] Kevin R. Cunningham, Bounded Rationality and Complex Process Coupling: Challenges for the Intelligence Support to Information Warfare, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 10 April 2000), 9.

[94] Chris C. Demchak, Military Organizations, Complex Machines: Modernization in the U.S. Armed Services (Ithaca, N.Y.: Cornell University Press, 1991), 100. Demchak makes this same conclusion in this book when she describes the complexities associated with fielding the M1 Abrams tank to the Army.

LIST OF ACRONYMS

ABCS- Army Battle Command System

ACAT- Army Acquisition Category

ACTD- Advanced Technologies Demonstrations

ACUS-MOD- Area Common User System-Modernization

AFATDS- Advanced Field Artillery Tactical Data System

AMDPCS- Air and Missile Defense Planning and Control System

ARFOR- Army Forces

ASAS- All Source Analysis System

ATM- Asynchronous Transfer Mode

AWE- Advanced Warfighting Experiment

C2- Command and Control

CBO- Congressional Budget Office

CINC- Commander in Chief

CONUS- Continental United States

COP- Common Operating Picture

COTS- Commercial Off the Shelf

CQB- Close Quarter Combat

CQM- Close Quarter Marksmanship

CRD- Capstone Requirements Document

CS- Combat Support

CSIS- Center For Strategic and International Studies

CSS- Combat Service Support

CSSCS- Combat Service Support Control System

DII- Defense Information Infrastructure

DTSS- Digital Topographic Support System

EPLRS- Enhanced Position Location Reporting System

FBCB2- Force XXI Battle Command Brigade and Below

FDD- First Digitized Division

FUE- First Unit Equipped

GBS- Global Broadcast System

GCCS-A- Global Command and Control System-Army

HTML- Hypertext Markup Language

HTTP- Hypertext Transfer Protocol

IAV- Interim Armored Vehicle

IBCT- Interim Brigade Combat Team

IMETS- Integrated Meteorological System

INC- Internet Controller

IOC- Initial Operational Capability

ISYSCON- Integrated System Control

JTA- Joint Technical Architecture

JTF- Joint Task Force

MCS- Maneuver Control System

MDMP- Military Decision Making Process

MOUT- Military Operations in Urban Terrain

MSE- Mobile Subscriber Equipment

MTW- Major Theater of War

NCA- National Command Authority

NCW- Network Centric Warfare

NIPRNET- Non-secure Internet Protocol Router Net

NOC-V- Network Operations Center

NTC- National Training Center

ODISC4- Office of the Director of Information Systems for Command, Control, Communications, and Computers

O&M- Operations and Maintenance

OPTEMPO- Operating Tempo

PCW- Platform Centric Warfare

RDTE- Research, Development, Testing, and Evaluation

RSTA- Reconnaissance, Surveillance, and Target Acquisition

SINCGARS- Single Channel Ground to Air Radio System

SMART-T- Secure, Mobile, Anti-jam, Reliable, Tactical Terminal

SSC- Small Scale Contingency

SWLAN- Secure Wireless Local Area Network

TCP/IP- Transmission Control Protocol/Internet Protocol

THSDN- Tactical High Speed Data Network

TOC- Tactical Operations Center

TRI-TAC- Tri-Services Tactical

TTP- Tactics, Techniques, and Procedures

UAV- Unmanned Aerial Vehicle

VTC- Video Tele-conferencing, or BVTC- Battlefield Video-teleconferencing

WMD- Weapons of Mass Destruction

BIBLIOGRAPHY

Alberts, David S. The Unintended Consequences of Information Age Technologies. Available from <http:/www.dodccrp.org/ucHome.htm>. Internet. Accessed 5 February 2001.

———, and Daniel S. Papp. The Information Age: An Anthology on Its Impacts and Consequences, Volume 1, Part One: The Information and Communications Revolution. Washington, D.C.: National Defense University Press, 1997.

———, John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, D.C.: DoD C4ISR Cooperative Research Program, August 1999.

Bender, Bryan. "Miniaturization." Jane's Defence Weekly, 25 October 2000.

Blaine, John M. First Digitized Division: The Challenges in Realizing the Tactical Internet. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 10 April 2000.

———. "First Digitized Division Challenges." Briefing slides with notes. Office of the Director for Command, Control, Communications, and Computers, Department of the Army, February 2000.

Caldera, Louis and Eric K. Shinseki. United States Army Transformation Campaign Plan. Washington, D.C.: Department of the Army, 27 October 2000.

Campbell, William H. "Force XXI...What You Can Expect to See." Briefing Slides. Director of Information Systems for Command, Control, Communications, and Computers, Department of the Army, June 2000.

———. "DISC4 Overview Briefing to Mr. Dahlberg." Briefing Slides. Director of Information Systems for Command, Control, Communications, and Computers, Department of the Army, no date.

Caneva, Joseph W. Network-Centric Warfare: Implications For Applying the Principles of War. Newport, R.I.: Naval War College, 17 May 1999.

Cebrowski, Arthur K. and John Garstka. "Network Centric Warfare: Its Origin and Future." Naval Institute Proceedings, January 1998. Available from <http://www.usni.org/Proceedings/Articles 98/Procebrowski.htm>; Internet. Accessed 5 February 2001.

Clinton, William J. A National Security Strategy For A New Century. Washington, D.C.: The White House, October 2000.

Cohen, William S. Annual Report to the President and the Congress. Washington, D.C.: U.S. Government Printing Office, 2000.

Cunningham, Kevin R. Bounded Rationality and Complex Process Coupling: Challenges for the Intelligence Support to Information Warfare. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 10 April 2000.

Demchak, Chris C. Military Organizations, Complex Machines: Modernization in the U.S. Armed Services. Ithaca, N.Y.: Cornell University Press, 1991.

Dixon, Patrick. "Poor Nations React to Globalization." Available from <http://www.globalchange.com/globalis.htm>. Internet. Accessed 15 January 2001.

Downes, Larry and Chunka Mui. Unleashing the Killer App: Digital Strategies for Market Dominance. Boston, MA: Harvard Business School Press, 2000.

Flowers, Jack D. Digitization of the Heavy Maneuver Brigade: Increased Situational Awareness and Decreased Decision Making. Available from <https://calldbpub.leavenworth.army.mil/>; Internet. Accessed 1 February 2001.

Friedman, Thomas L. The Lexus and the Olive Tree. New York, NY: Anchor Books, April 2000.

Gouré, Daniel and Jeffrey M. Ranney. Averting the Defense Train Wreck in the New Millennium. Washington, D.C.: The CSIS Press, November 1999.

Gerstein. "Army Transformation Information Paper." DAMO-SSV, Department of the Army, 5 September 2000.

Hall, Wayne. The Janus Paradox: The Army's Preparation for Conflicts of the 21st Century. Arlington, VA: The Institute of Land Warfare, Association of the United States Army, October 2000.

Hamilton, Brian and Walter Brown. "Tactical High Speed Data Network: The Interim Army's Answer to Battlefield Data Transport." Available from <http://www.gordon.army.mil/regtmktg/AC/SPR00/thsdn.htm>; Internet. Accessed 25 January 2001.

Henry, Ryan and C. Edward Peartree. The Information Revolution and International Security. Washington, D.C.: The CSIS Press, 1998.

Joint Publication 3-0. Doctrine For Joint Operations. Washington, D.C.: The Joint Chiefs of Staff, 1 February 1995.

Joint Publication 3-13. Joint Doctrine For Information Operations. Washington, D.C.: The Joint Chiefs of Staff, 9 October 1998.

Joint Staff Brochure. Information Warfare: A Strategy for Peace...The Decisive Edge in War. Washington, D.C.: The Joint Chiefs of Staff, 7-8.

Koch, Andrew. "Joining the Force." Jane's Defence Weekly, 25 October 2000.

Macgregor, Douglas A. Breaking the Phalanx: A New Design for Landpower in the 21st Century. Westport, CT: Praegor Publishers, 1997.

Mendelas, Mark D. Organizational Structure to Exploit the Revolution in Military Affairs. Fairfax County, VA: January 2000.

National Defense Panel. Transforming Defense, National Security in the 21st Century. Washington, D.C.: U.S. Government Printing Office, December 1997.

Newton, Harry. Newton's Telecom Dictionary. New York, NY: Miller Freeman, Inc., August 1999.

Roper, Daniel. "Technology: Achilles' Heel or Strategic Vision?" Military Review, March–April 1997. Available from <http://www-cgsc.army.mil/milrev/milrvweb/html>; Internet. Accessed 25 January 2001.

Seena, Simon. "Pentagon Report Cites Sagging Airlift." Army Times, 29 January 2001.

———. "Lighter, Faster Forces Depend on Air Force Airlift Makeover." Army Times, 29 January 2001.

Shalikashvili, John M. Shape, Respond, Prepare Now: A Military Strategy for a New Era. Washington, D.C.: The Joint Chiefs of Staff, 1997.

Shelton, Henry H. Joint Vision 2020. Washington, D.C.: The Joint Chiefs of Staff, June 2000.

Shinseki, Eric K. The Army Vision. Washington, D.C.: U.S. Department of the Army, 1999.

———. "The Army Transformation: A Historic Opportunity." Army, October 2000, p. 28.

Tabler, Anthony D. and Thomas Nugent. "Project Manager Warfighter Information Network-Terrestrial Two Star Review." Briefing Slides. Fort Gordon, GA: U.S. Army Signal Center, 14 November 2001.

The Institute of Land Warfare. Fiscal Year 2001, Army Budget and Analysis. Arlington, VA: Association of the United States Army, July 2000.

The Institute of Land Warfare. Profile of the Army, a Reference Handbook. Arlington, VA: Association of the United States Army, February 1997.

The Institute of Land Warfare. Army Report: Research and Development:: Enabling Transformation. Arlington, VA: Association of the United States Army, October 2000.

U.S. Army War College. How the Army Runs: A Senior Leader Reference Handbook. Carlisle Barracks, PA: U.S. Army War College, 1999-2000.

U.S. Army Combined Arms Center. "Army Battle Command System Capstone Requirements Document Revision 1c." Fort Leavenworth, KS: TRADOC Program Integration Office Army Battle Command System, 3 October 2000.

U.S. Army, Department of the Army. Weapon Systems. Washington, D.C.: U.S. Government Printing Office, 2000.

U.S. Army. Directorate of Army Integration. Army Digitization Master Plan. Washington, D.C.: Department of the Army, 1996.

U.S. Army. Director, Combat Developments. The Brigade Combat Team Organizational and Operational Concept. Fort Monroe, VA: U. S. Army Training and Doctrine Command (TRADOC), 22 February 2000.

U.S. Army. Director of Command, Control, Communications, and Computers (ODISC4). Joint Technical Architecture-Army Version 5.5. Washington, D.C.: Department of the Army, 23 December 1998.

U.S. Army. Financial Management and Comptroller. The Army Budget, FY01 President's Budget. Washington, D.C.: U.S. Department of the Army, 2000.

U.S. Army. FM 11-43, The Signal Leader's Guide. Washington, D.C.: Department of the Army, 12 June 1995.

U.S. Army. Office of the Director, Information Systems for Command, Control, Communications, and Computers. Digitized Force Systems Architectures: Blueprints for a Force XXI Army. CD-ROM v3.0. Washington, D.C.: Department of the Army, 30 March 2000.

U.S. Army. Training and Doctrine Command (TRADOC). "The Foundations of Army Transformation and the Objective Force Concept Final Draft." Fort Monroe, VA: 16 December 2000.

U.S. Congress. Congressional Budget Office. Budgeting for Defense: Maintaining Today's Forces. 106th Cong., 2d sess., September 2000.

U.S. General Accounting Office. Battlefield Automation: Performance Uncertainties Are Unlikely When Army Fields Its First Digitized Division. Washington, D.C.: U.S. General Accounting Office, July 1999.

U.S. Senate. Committee on Armed Services. Full Committee. Testimony on the Status of U.S. Military Readiness. 106th Cong., 2d sess., 27 September 2000.

Zakaria, Fareed. "The New Twilight Struggle." Newsweek, 23 October 2000, p. 37.